REMARKS

Claim 1-18 were examined by the Office, and in the Office Action of August 21, 2007 all claims are rejected. With this response claims 7-10 are amended to remove "step of" language, and to place the claims in better form. All amendments are fully supported by the specification as originally filed.

Applicant respectfully requests reconsideration and withdrawal of the rejections in view of the following discussion.

Claim Rejections Under § 102

In section 3, on page 2 of the Office Action, claims 1, 3-4, 7, 9-10, 13 and 15-16 are rejected under 35 U.S.C. § 102(e) as anticipated by Braithwaite (U.S. Patent No. 6,724,554). Applicant respectfully submits that Braithwaite fails to disclose or suggest independent claim 1, because Braithwaite fails to disclose or suggest all of the limitations recited in claim 1. Braithwaite at least fails to disclose or suggest at least one storage area in a storage circuit, in which protected data relating to circuitry security is located in the storage area, as recited in claim 1. Braithwaite also fails to disclose or suggest mode setting means arranged to set a processor in one of at least two different operating modes, wherein in a first processor operating mode the processor is enabled to access the storage area, and in a second processor operating mode the processor is prevented from accessing the storage area in which protected data is located, as recited in claim 1.

The present invention relates to the idea that circuitry is provided in which a processor is operable in at least two different modes, one first secure operating mode and one second unsecure operating mode. In the secure mode, the processor has access to security related data, i.e. protected data relating to circuitry security as recited in claim 1, located in various memories located within the circuitry. The security data includes cryptographical keys and algorithms, software for booting the circuitry, secret data such as random numbers used as cryptographical key material or application programs. The access to these security data and the processing of them needs to be restricted, since an intruder with access to security data could manipulate a device, for example a mobile terminal, in which the circuitry of the present invention is implemented. When testing and/or debugging the terminal, access to the security data is not

allowed. For this reason, the processor is placed in the unsecure operating mode, in which mode it is no longer given access to the security data. The present invention advantageously enables the processor of the circuitry to execute non-verified software downloaded into the circuitry. This allows testing, debugging and servicing of the electronic device and its software without risking that a third party is given access to information which makes it possible to manipulate the security related components of the device so as to affect the security functions when in the secure environment.

In contrast to the present invention as recited in claim 1, Braithwaite generally discloses a method of inhibiting inadvertent and unauthorized writing and reading of information to and from a removable storage medium, and more particularly a removable disk cartridge. The method includes writing codes in a predetermined location of the storage medium. In Braithwaite, the storage medium (60) is subject to one of four different protection modes, and each protection mode specifies a different way in which access to the data tracks (62) of the storage medium may be inhibited. See Braithwaite column 5, lines 22-26. For example, in the Unlock Mode the storage medium has no read or write protection, and in the Write Protect Mode the storage medium is write-protected. See Braithwaite column 5, lines 28-35. However, in Braithwaite it is the mode of the storage medium that is set, and in contrast to claim 1, Braithwaite does not disclose or suggest setting a mode of the microprocessor (92).

The microprocessor merely controls access to the storage medium in accordance with the protection mode set for the storage medium. See Braithwaite column 7, lines 56-60. The mode for the microprocessor is not set, but rather the microprocessor is merely responsible for executing the protection mode command set for the storage medium. See Braithwaite column 8, lines 61-65. Therefore, Braithwaite only discloses a number of modes which are all concerned with the protection mode of the storage, not the operating mode of the processor, as recited in claim 1. As described above, the processor in claim 1 can be set in a first and a second operating mode. In the first operating mode, the processor has access to the protected data located in the storage area within the circuitry. When the processor is placed in the second operating mode, it is no longer given access to the protected data within the circuitry. However, Braithwaite fails to disclose or suggest different processor operating modes, as recited in claim 1. Therefore, for at least this reason, claim 1 is not disclosed or suggested by Braithwaite.

Furthermore, Braithwaite also fails to disclose or suggest that protected data relating to circuitry security is located in the storage area of the storage circuit, as recited in claim 1. While Braithwaite states that any data may be stored in the storage medium (60), there is no mention or suggestion that this data may be protected data related to circuitry security. Therefore, for at least this additional reason claim 1 is not disclosed or suggested by Braithwaite.

In addition, Braithwaite makes no mention or suggestion that in a second processor operating mode the processor is enabled to execute non-verified software downloaded into the circuitry, as recited in claim 1. Instead, Braithwaite only addresses modes with respect to read and write protection of the storage medium (60), and does not even disclose or suggest that non-verified software may be executed in one mode but not another, since Braithwaite makes no mention or suggestion of executing non-verified software on the storage medium. Therefore, for at least the reasons discussed above, claim 1 is not disclosed or suggested by Braithwaite.

Independent claims 7 and 13 contain limitations similar to those recited in claim 1, and are rejected for the same reasons as claim 1. Therefore, for at least the reasons discussed above in relation to claim 1, claims 7 and 13 are not disclosed or suggested by Braithwaite.

The dependent claims depending from the above mentioned independent claims are also not disclosed or suggested by Braithwaite at least in view of their dependencies.

Claim Rejections Under § 103

In section 8, on page 3 of the Office Action, claims 2, 6, 8, 12, 14 and 18 are rejected under 35 U.S.C. § 103(a) as unpatentable over Braithwaite in view of Sato (U.S. Appl. Publ. No. 2001/0055980). Applicant respectfully submits that the claims rejected above all ultimately depend from an independent claim, and therefore are not disclosed or suggested by the cited references at least in view of their dependencies.

In section 11, on page 4 of the Office Action, claims 5, 11 and 17 are rejected under 35 U.S.C. § 103(a) as unpatentable over Braithwaite in view of Ishidera (U.S. Appl. Publ. No. 2002/0040442). Applicant respectfully submits that the claims rejected above all ultimately depend from an independent claim, and therefore are not disclosed or suggested by the cited references at least in view of their dependencies.

Conclusion

It is respectfully submitted that the present application is in condition for allowance, and such action is earnestly solicited. The undersigned hereby authorizes the Commissioner to charge Deposit Account No. 23-0442 for any fee deficiency required to submit this response.

Respectfully submitted,

Date: 8 November 2007

s/Keith R. Obert/
Keith R. Obert
Attorney for the Applicant
Registration No. 58,051

KRO/kas
WARE, FRESSOLA, VAN DER SLUYS
& ADOLPHSON LLP
755 Main Street, P.O. Box 224
Monroe, Connecticut 06468
Telephone:(203) 261-1234
Facsimile: (203) 261-5676
USPTO Customer No. 004955